Enterprise Risk Management Framework education

Audits and Risk Management Committee

March 2024

Purpose

Risk management is **a process** designed to identify potential events and manage risks, to provide reasonable assurance regarding the achievement of business objectives.

Definition

An **enterprise risk management (ERM) framework** is the set of policies, procedures, activities and tools used to effectively identify, assess and manage risks.

Governance documents

- Board risk management policy
- ARM Committee charter
- ERM program charter
- ERM framework graphic
- Executive Risk and Compliance Committee (ERCC) charter
- Risk champion network charter
- ERM policy

ERM framework principles

Governance & Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Review & Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues improvement in Enterprise Risk Management

Information, Communication, & Reporting

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

Source – COSO Enterprise Risk Management. www.coso.org

ERM Framework

CalSTRS Enterprise Risk Management Framework

Component 1: GOVERNANCE

Teachers' Retirement Board
The trustees have ultimate responsibility and accountability for risks.

Executive Risk and Compliance Committee
ERM Program oversight and clearinghouse for risk policy, appetite-setting and governance.

Component 2: PEOPLE, PROCESS, DATA AND TECHNOLOGY

Business Area Risk Owners (Risk Champions, Managers & Staff)	**Aligned Assurance Groups** (ERM, ECS, Information Security)	**Internal and External Audits**
Identifies and take actions to reduce risks.	Provides expertise, support, analysis and reports on the management of risks to the board, ERC and CalSTRS senior management.	Provides independent assurance to the board and CalSTRS senior management on risk management.

Component one: Governance board oversight

- The Teachers' Retirement Board **establishes the organization's tone and culture** towards effective risk management and maintains oversight of CalSTRS approach to risk management.
- The Board Governance Manual ***Risk Management Policy*** states that the board shall establish CalSTRS:
  - Risk oversight framework and reporting metrics.
  - Commitment to periodic review and verification of the risk management policy.
  - Risk appetite or aversion and rationale for managing risk.
  - Accountabilities and responsibilities for managing risk.

The ARM Committee has been established to **assist the board** in fulfilling its fiduciary oversight for the ERM Framework, compliance, financial reporting, internal controls, internal audit and external audit engagements.

Component one: governance

Executive Risk and Compliance Committee (ERCC)

- Executive committee chaired by the CFO and co-chaired by the COO.
- Chief Auditor, Communications Director, Human Resources Director, Information Security Officer, and Strategy Director serve in a consultative role.
- Responsibilities include:
  - Establishing a risk-aware culture throughout CalSTRS.
  - Providing ongoing guidance and support to the ERM team.
  - Ensuring the accurate, timely and consistent flow of risk management information to the Teachers' Retirement Board.
  - Ensuring procedures, processes and controls are in place and maintained for the enterprise-wide management of CalSTRS' key risks.

Component one: governance reporting

Teachers' Retirement Board

- Semi-Annual risk report
- CEO Report on emerging risks

Audits and Risk Management Committee

- Enterprise Compliance Services workplans

Executive Risk and Compliance Committee

- Emerging risk reports
- Risk matrix reports
- Enterprise Compliance Services workplans
- Policy updates

ERM Framework

CalSTRS Enterprise Risk Management Framework

Component 1: GOVERNANCE

Teachers' Retirement Board
The trustees have ultimate responsibility and accountability for risks.

Executive Risk and Compliance Committee
ERM Program oversight and clearinghouse for risk policy, appetite-setting and governance.

Component 2: PEOPLE, PROCESS, DATA AND TECHNOLOGY

Business Area Risk Owners (Risk Champions, Managers & Staff)	**Aligned Assurance Groups** (ERM, ECS, Information Security)	**Internal and External Audits**
Identifies and take actions to reduce risks.	Provides expertise, support, analysis and reports on the management of risks to the board, ERC and CalSTRS senior management.	Provides independent assurance to the board and CalSTRS senior management on risk management.

Component two: people

Business area risk owners

- Risk champions
- Management and staff

Aligned assurance groups

- Enterprise Risk Management
- Enterprise Compliance Services
- Information Security Office

Internal and external audits

- Audit Services (internal)
- Crowe (external)

Component two: process

Risk identification

- Enterprise level risk identification
- Emerging risks
- Existential risks
- Branch risk assessment

Component two: process

Risk response

CalSTRS recognizes various **responses to manage risks** within the ERM Framework.

- Accept
- Share
- Reduce
- Avoid

Component two: process

Component two: data and technology

Enterprise Risk and Compliance maturity plan includes acquiring and implementing software for streamlining and enhancing risk processes.

ERM Framework

CalSTRS Enterprise Risk Management Framework

Component 1: GOVERNANCE

Teachers' Retirement Board
The trustees have ultimate responsibility and accountability for risks.

Executive Risk and Compliance Committee
ERM Program oversight and clearinghouse for risk policy, appetite-setting and governance.

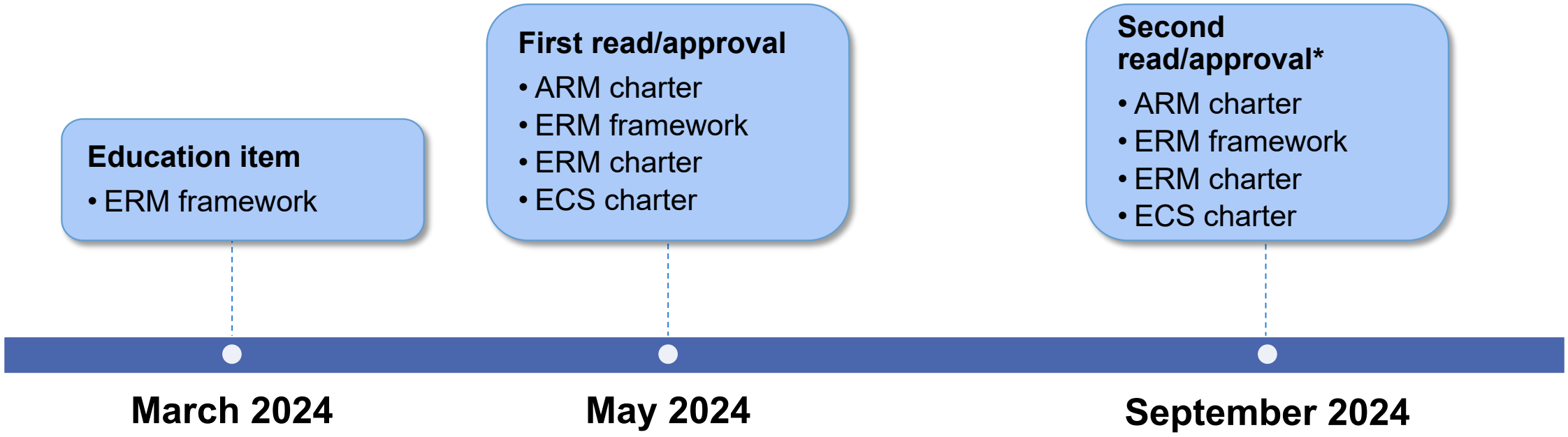
Component 2: PEOPLE, PROCESS, DATA AND TECHNOLOGY

Business Area Risk Owners (Risk Champions, Managers & Staff)	**Aligned Assurance Groups** (ERM, ECS, Information Security)	**Internal and External Audits**
Identifies and take actions to reduce risks.	Provides expertise, support, analysis and reports on the management of risks to the board, ERC and CalSTRS senior management.	Provides independent assurance to the board and CalSTRS senior management on risk management.

ERM Framework: next steps

- Integrating enterprise strategy into framework documents
- Integrating enterprise compliance into framework documents
- Bringing documents to the Executive Team and ARM Committee for feedback and approval

ARM Committee: Framework update timeline



*If second read needed.